PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G11B 23/28, 23/36, 23/40	A1	(11) International Publication Number: **WO 00/36605**
		(43) International Publication Date: 22 June 2000 (22.06.00)

(21) International Application Number: PCT/SG98/00104

(22) International Filing Date: 11 December 1998 (11.12.98)

(71) Applicant *(for all designated States except US)*: KENT RIDGE DIGITAL LABS [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

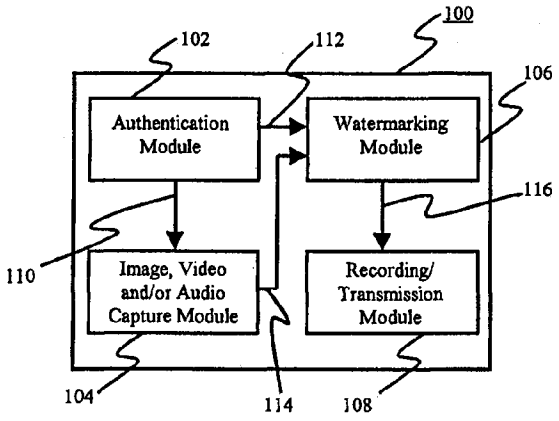
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: WU, Jian, Kang [CN/SG]; Blk 51 Teban Gardens Road, #06–605, Singapore 600051 (SG). NARASIMHALU, A., Desai [IN/SG]; 103 Clementi Road, #03–01, Kent Vale, Singapore 129788 (SG). LO, Sheng [SG/SG]; Blk 444, Jurong West Avenue 1, #11–774, Singpaore 640444 (SG). LEBRUN, Jean–Luc [FR/SG]; 10G Braddell Hill, #23–27 Braddell View, Singapore 579726 (SG).

(74) Agent: SPRUSON & FERGUSON PTE LTD.; 51 Bras Basah Road, #02–03 Plaza by the Park, Singapore 189554 (SG).

(81) Designated States: GB, SG, US.

Published
With international search report.

(54) Title: METHOD AND DEVICE FOR GENERATING DIGITAL DATA WATERMARKED WITH AUTHENTICATION DATA



(57) Abstract

An apparatus (100), method and computer program product for generating an authenticated audio, image and/or video signal (116) is disclosed. The apparatus or recording device (100) includes an authentication module (102), an audio, image and/or video capture module (104), and a watermarking module (106). The apparatus can be a digital camera, digital video camera, or a digital audio recording device. The authentication module (102) checks if the operator is authorized to use the apparatus (100) and if so generates authentication information (112). Biometrics data such as a fingerprint, iris, voice and/or face recognition can be used for authentication. If authorized, the capture module (104) generates an audio, image and/or video signal (114). A watermarking module (106) embeds the authentication information (112) in the media signal (114) to provide the authenticated output signal (116). The watermarking is built into the recording device (100) and is carried out on–the–fly. The media signal can be watermarked with GPS data and/or annotation.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND DEVICE FOR GENERATING DIGITAL DATA WATERMARKED WITH AUTHENTICATION DATA

FIELD OF THE INVENTION

The present invention is directed to the field of recording digital audio, image and/or video signals and, in particular, to a method and apparatus for embedding information in digital audio, image and/or video signals.

BACKGROUND

The subsistence of copyright in artistic works is a significant and valuable right rewarding artistes for their original, creative efforts. Amongst other things, the subsistence of copyright in an artistic work allows a copyright owner to advantageously commercially exploit their work and also to control the use and treatment of such artistic works by others. The existence of copyright is particularly important in relation to artistic works in fields such as photography, music and film.

In conventional photography and other image acquisition processes, claims of ownership in photographs and similar image recordings are typically indicated by manually labeling the back of the photographs with details of the owner. Alternatively, stickers or rubber stamps may be used to mark the photographs. However, such methods do not provide incontrovertible or substantially incontrovertible evidence of ownership of the artistic work by the owner. For example, a false claim of ownership can be made on unmarked materials owned by another, can be defaced or erased, or can be overwritten with false markings of another claimant.

In film and video recordings, ownership rights are frequently made by adding details of the owner in a header and/or a trailer portion of the recording. For audio recordings, ownership details are normally indicated on the recording media (e.g., CD-ROM, tape, etc.) or packaging. However, ownership indicia are capable of being easily removed or altered from the recordings or packaging.

With the widespread advent of digital recording technology, artistic works can be readily duplicated and distributed worldwide immediately by communication channels like the Internet, Intranets, and satellite communications. Further, such digital artistic works are readily susceptible of unauthorised modification and tampering. The recording of an artistic work in the digital domain exacerbates the problems of establishing ownership of copyright in an artistic work. Several techniques have been attempted to address this issue.

United States Patent No. 5,513,260 discloses a method and apparatus that attempts to provide copyright protection for recording media such as compact discs (CDs) using encryption. In particular, a combination of symmetrical and asymmetrical data encryption is used to permit a reproduction device to handle either copy-protected or non-copy-protected media. The technique encrypts the digital recording on a recording media. However, the system does not directly relate the artistic work contained in the recording with the copyright owner, and a digital recording once decrypted can be copied or modified without any protection for the copyright owner.

United States Patent No. 4,890,319 discloses a subscription television system for distributing copyrighted program material to subscribers. The system has a transmitter with a data-insertion circuit for inserting a control bit in a transmitted signal, which comprises other control data and the copyrighted program material. A receiver in the system includes a memory for storing a pre-assigned subscriber identification. Upon receipt and identification of the control bit at the receiver, the receiver inserts a subscriber identification into the program material. An unauthorized copy of the program material may be determined since it includes the subscriber identification. However, again, the system does not directly relate the artistic work itself contained in the recording with the copyright owner, and a party familiar with the system can defeat the system by appropriate processing to remove the subscriber identification.

The foregoing systems are disadvantageous in that they fail to uniquely relate the content of the artistic work itself with the owner in a manner that effectively prevents

tampering. Further, the systems cannot ensure that the recordings to which the techniques are applied are the property of the party asserting ownership.

SUMMARY

The aspects of the invention are directed to ameliorating or overcoming one or more disadvantages of conventional systems including those described above. The aspects of the invention are able to do so by requiring authentication data derived from an authorised operator to operate a recording device and providing on-the-fly copyright ownership indicia in a recording, when recording, by watermarking the recording using the authentication data.

In accordance with a first aspect of the invention, a method of generating an authenticated audio, image and/or video signal is disclosed. The method includes the steps of generating an authentication signal, capturing a digital audio, image and/or video signal, and watermarking the digital audio, image audio, image and/or video signal using the authentication signal to provide the authenticated audio, image and/or video signal.

Preferably, the method further includes the steps of: determining if an operator is authorised to generate the authenticated audio, image and/or video signal; and if so, enabling capture of the digital audio, image and/or video signal.

Preferably, the step of generating the authentication signal is performed substantially simultaneously with the step of capturing the digital audio, image and/or video signal. Further, the authentication signal can be derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

Optionally, the step of capturing the digital audio, image and/or video signal includes: capturing an analog audio, image and/or video signal; and converting the analog audio, image and/or video signal to the digital audio, image and/or signal.

Also, the watermarking step provides perceptible and/or non-perceptible watermarks. Optionally, the method includes annotating the digital audio, image and/or video signal using text and/or audio data. The annotation can be persistent and/or non-persistent.

In accordance with a second aspect of the invention, an apparatus for generating an authenticated audio, image and/or video signal is disclosed. The apparatus includes: a module for generating an authentication signal; a module for capturing a digital audio, image and/or video signal; and a module for watermarking the digital audio, image and/or video signal using the authentication signal to provide the authenticated, copyrighted audio, image and/or video signal.

Preferably, the apparatus further includes: a module for determining if an operator is authorised to generate the authenticated audio, image and/or video signal; and a module for enabling capture of said digital audio, image and/or video signal in response to determining the operator is authorised.

Preferably, the module for capturing the digital audio, image and/or video signal operates substantially simultaneously with the module for generating the authentication signal. Further, the authentication signal can be derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

Optionally, the module for capturing the digital audio, image and/or video signal includes: a module for capturing an analog audio, image and/or video signal; and a module for converting the analog audio, image and/or video signal to the digital audio, image and/or signal.

Also, the watermarking module provides perceptible and/or non-perceptible watermarks. Optionally, the apparatus includes a module for annotating the digital

audio, image and/or video signal using text and/or audio data. The annotation can be persistent and/or non-persistent.

In accordance with a third aspect of the invention, a computer program product having a computer readable medium having a computer program recorded therein for generating an authenticated audio, image and/or video signal is disclosed. The computer program product includes: means for generating an authentication signal; means for capturing a digital audio, image and/or video signal; and means for watermarking the digital audio, image and/or video signal using the authentication signal to provide the authenticated audio, image and/or video signal.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention are described hereinafter with reference to the drawings, in which:

Figure 1 is a block diagram of an apparatus for generating an authenticated audio, image and/or video signal in accordance with a first embodiment of the invention;

Figure 2 is a flowchart illustrating a method of generating an authenticated audio, image and/or video signal in accordance with a second embodiment of the invention; and

Figure 3 is a block diagram of an apparatus for generating an authenticated audio, image and/or video signal in accordance with a third embodiment of the invention;

DETAILED DESCRIPTION

A method, apparatus and computer program product for generating an authenticated audio, image and/or video signal, where the authenticated signal is an audio, image and/or video signal watermarked with authentication data, are described. In the following description of several embodiments, numerous specific details such as particular watermarking techniques are described in order to provide a more thorough

description of those embodiments. It will be apparent, however, to one skilled in the art that the present invention may be practiced without those specific details. In other instances, well-known features such as particular video formats (e.g. MPEG), particular biometrics data, for example, have not been described in detail so as not to obscure the invention.

In broad terms, the embodiments of the invention provide a mechanism for providing a robust, tamper-evident "stamp" of authorship and/or ownership of audio, image and video works. This is done by requiring authentication data to operate an audio, image and/or video-recording device and providing on-the-fly copyright ownership indicia in an audio, image and/or video recording, when recording, by watermarking the recording using the authentication data. The authenticated watermarking is used to verifiably establish the subsistence of copyright ownership of the audio, image and/or video materials.

In the embodiments of the invention, both the generation of authentication data specific to the owner or operator of the recording device and the watermarking are implemented as components of the recording device. Amongst other things, this overcomes disadvantages of the prior art where watermarking might be implemented as an external post-processing procedure on a work downloaded or retrieved from a recording device at one point in time and then watermarked at a later point. In such circumstances, the presence of an original un-watermarked audio, image and/or video work external to the recording device provides opportunities for further disputes in the authenticity of the images. This might occur for example where a third party obtained a copy of the original un-watermarked audio, image and/or video work and watermarked it with data indicating that it was their property. In such circumstances, both the proper owner and the third party would have watermarked copies of the original work with conflicting claims of authorship and/or ownership.

The embodiments of the invention embed watermarking technology directly into the audio, image and/or video acquisition process as a means of protecting intellectual

property rights in the acquired work. In particular, one embodiment directly embeds the watermarking module into the hardware of the recording or acquisition device. Such an arrangement can render every segment of captured media via the recording device to bear the desired digital signature and/or caption embedded by the watermarking module.

For example, when a digital photo or a video segment is taken, immediately there can be potential copyright and annotation issues. Examples of persons affected by such issues include professional journalists and film producers. The embodiments of the invention significantly reduce and potentially eliminate conflicts regarding copyright authorship and ownership if the photo and video, for example, are watermarked with authenticated information specific to the journalist and film producer as soon as they are created. With a properly watermarked photo, the journalist can safely send it to the person's news agent and other news agents with significantly less concern that such persons might successfully assert an improper claim of copyright and/or ownership of the work. Since the audio, image and/or video work is in digital form, it can be easily indexed, stored in a data storage device, and transmitted over a network.

To prevent unauthorized access of the camera/recorder and unauthorized use of data captured by the camera/recorder, an authentication module is included in the camera/recorder to control operation of the camera/recorder. The authentication module may implement any of a number of authentication techniques such as: biometrics data including fingerprints, voice, and face of an authorised operator; a removable smart card containing encoded or encrypted data specific to the authorised operator; a password known by the authorised operator, etc. Alternatively, access data may be transmitted from a remote device such as radio, infrared or other appropriate transmitter acting as a security key of sorts. The authentication module further serves to enforce the authenticity of the recording equipment. The embodiments of the invention can be implemented to render the recording equipment useless in the event of theft, for example.

Optionally, the embodiments of the invention may also incorporate encryption and scrambling techniques, which are widely used in relation to digital photographs, video, and audio to protect them from unauthorized usage. Still further, the embodiments may incorporate an annotation module for annotating an audio, image and/or video work with text and/or audio information, for example. Optionally, the embodiments of the invention implement persistent annotation using watermarking and on-line annotation using voice.

A block diagram of a recording device according to a first embodiment of the invention is depicted in Fig.1. The device 100 for generating an authenticated audio, image and/or video signal includes an authentication module 102, an image, video and/or audio capture module 104, and a watermarking module 106 as its principal features. It also includes a recording/ transmission module 108 for recording and/or transmitting the authenticated audio, image and/or video signal containing embedded watermarks. The authentication module 102 is used to determine whether or not an attempted operator of the device 100 is an authorized user. It is also used to obtain and determine authentication information 112, which is subsequently watermarked in the capture audio, image and/or video work. The capture module 104 can be a type of digital camera, video camera or audio recorder. The watermarking module 106 embeds the authentication information 112 into the digital media 114 to provide the authenticated audio, image and/or video signal 116. Again, this is done to indicate copyright authorship and/or ownership of the audio, image and/or video work.

In particular, the authentication module 102 provides an enabling/disabling signal 110 to the image, video and/or audio capture module 104 dependent upon the results of checking if the attempted operator is authorised to use the device 100. For example, if the authentication module 102 determines that the attempted operator is authorised to operate the device 100, it generates an enable signal 110 which can actuate the image, video and/or audio capture module 104 to generate a relevant signal. Conversely, the authentication module 102 can disable 110 the capture module 104 if the attempted operator is not authorised.

The authentication module 102 protects usage of the device 100 as well as creation of authentication information 112. Authentication can be implemented in any of a number of ways. The simplest is to require the operator to input a password, perhaps using a keypad, to the recording device 100. Another way of implementing authentication is to require the user to swipe an encoded magnetic card through a card reader built in as part of the recording device 100. Alternatively, the device 100 can be adapted to receive an electronically readable card such as a smart card serving as a token that the authentication module 102 can check. Perhaps, the most secure way is to use a device for capturing biometric data from the operator such as fingerprint, facial, or speech recognition. As an example, for the case where the recording device 100 is a digital camera, a transparent button may be used as the button for actuating the digital camera to capture an image in a conventional manner. The authentication module may include a sensor for capturing the fingerprint of the operator when the operator presses the camera actuation button. Alternatively, the sensor may be oppositely disposed in the body of the recording deive, such as at its bottom, where the operator might place a thumb when pressing the actuation button.

Prior to any other processing by the camera, the authentication module 102 can check the captured fingerprint against one or more authorised fingerprints stored in a storage device (e.g. an electronic memory, magnetic storage device, optical storage device,) forming part of the authentication module 102 to determine if the operator is authorised to use the camera. Another implentation may obtain a retinal scan of an eye of the operator as biometric data when the operator looks into the camera sight and presses the actuation button. Still another implementation may use speech recognition in respect of an audio recorder to actuate the recorder where the recorder is voice actuated. As specific details for obtaining biometric data and comparing them with stored data are well known, these details of the authentication module 102 are not set forth in further detail so as not to obscure the invention. Likewise the use of passwords, magnetic cards and electronic cards such as smart cards are well known and therefore these features are not set forth in greater detail.

Authentication carried out by the authentication module 102 can be performed when the operator starts using the recording device 100, and when the operator stops using it for a certain period. Alternatively, the authentication module 102 may require verification of the operator periodically during operation of the recording device 100. For example, for each shut of a digital camera, the authentication module 102, if implemented as an iris-recognition module or a fingerprint-recognition module, can be built in to verify automatically the operator when that person aims the digital camera at a target.

Preferably, default authentication information 112 is loaded each time an authorised operator starts using the recording device 100. Optionally, an editing function is provided to enable the operator to edit authentication information contained in or derived from the authentication module 102. The default authentication information 112 may include one or more of the following: the name of the owner of the recording device 100 or of the authorised operator, the organization relevant to the owner or operator, and the time and date. The foregoing authetication information is merely exemplary. Alone or in combination with other data, it may contain original biometric data such as information derived from the operator's fingerprint. As described hereinafter in relation to another embodiment of the invention hereinafter, the authentication information 112 may optionally include location data identifying the place where the media data is captured. The location may be automatically determined using the Global Position System (GPS).

As yet another example, a recording device 100 according to the first embodiment can be implemented as a high-end digital camera, which is owned by a journalist "John" who is the only authorised user of the camera. In the camera as purchased, a password can be set in the authentication module 102. John can use the password to access the camera 100 initially, change the password to be his fingerprint, and register himself as the only authorised user. He can also set the default authentication information 112 to include his full name, time and location when the picture is taken. The authentication

module 102 can include a small-size, solid-state fingerprint scanner (not shown) that can be well fitted readily to the body of the digital camera 100. When John holds the camera 100 ready to capture an image, his thumb is on the scanner. Without John noticing, when John is holding the camera and attempts to actuate the shutter button, the scanner captures his thumb print and the thumb print is processed by the authentication module 102 to extract minuature points from the scanned image. For detailed information about biometrics authentication, reference is made to Jain, A., Bolle, R., and Pankanti, S., BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, October 1998. The minuature points can then be matched by the authentication module 102 against ones captured and stored together with his name and other authentication information in a storage device of the capture module 102. The match can take account of the location, type, and orientation of those minuature points. The default authentication information 112 can be retrieved and sent to the watermarking module 106. If the authentication is not successful, operation of the camera shutter in the image capture module 104 is locked or inhibited.

For each individual operation of the recording device 100 or at predetermined instances in a continuous recording interval, the captured media data 114 output by the capture module 104 is watermarked automatically by the watermarking module 106 by embedding one or more watermarks into the media data 114. Preferably, each watermark is a non-perceivable signal. However, the watermarking module 106 can be implemented to embed perceivable watermarks. The embedded signal preferably contains the authentication information the user has edited. Any of a number of watermark techniques for image, audio and video signals may be practiced in the watermarking module 106. Preferably, the particular watermarking techniques to be practiced in the embodiments of the invention possess the following features: non-perceivable, robust, and tamper-proof. By "non-perceivable" is meant that there is no perceivable difference between an original and a watermarked media (i.e., audio, image and/or video signal). In other words, the watermarking process does not affect a predetermined level of humanly perceivable quality of the original media. By "robustness" is meant that an embedded watermark signal is not removable under

media processing and manipulation processes such as filtering, analog-to-digital (A/D) and digital-to-analog (D/A) conversion, and geometric transformations. By "tamper-proof" is meant that the ownership of the media is well-protected against attacks by others.

For additional security, the watermarked media signal can be scrambled/encrypted using a private key generated from the authentication information, for example, or directly from the biometrics data.

As a further optional feature, a database entry can be created in a storage medium of the recording device 100 to keep a record of watermarked media data. For law-enforcement purposes, amongst others, certain registration information contained in the database can be sent to an authority or a public service center, in a manner known to those skilled in the art. Similar techniques are used to register digital signatures via the Internet, for example. This registration information can later be used to verify the authorship and/or ownership of the audio, image and/or video work that has been watermarked with authentication data.

Again with reference to an implementation of the recording device 100 as a digital camera (the following applies equally to digital video and audio recording), after authentication that may be transparent to the operator, John identifies new scenery for image capture and presses the shutter button of the camera 100. Actuation of the button activates capture of a digital photo by the capture module 104 and watermarks the digital photo or image 114 with the authentication information 112 provided by authentication module 102. There are many image watermarking techniques available for such a digital photo application. For an exemplary watermarking technique, reference is made to Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T., Secure Spread Spectrum Watermarking for Multimedia, NEC Technical Report, 95-10. That watermarking technique can be used in this embodiment to convert the authentication information (e.g., the operator's identification) into signal patterns based on the concept of spread spectrum communication. The signal patterns are added to the

original image in the transform domain (e.g., digital cosine transform can be used). By doing so, the embedded watermark signal is spread over the whole image of the digital photo 114. It is therefore difficult to remove the watermark signal using ordinary image processing operations, making it strongly tamper-proof.

Further, the digital photo watermarked with the authentication data 116 output by the watermarking module 106 can be recorded on a storage medium or transmitted to an external location by the recording/transmission module 108.

The recording/transmission module 108 can include storage media such as electronic, magnetic, optical and/or magneto-optical storage media, which can be implemented as removable or non-removable storage media. As an illustrative example, the media can be a removable storage medium such as a floppy disc, which is used in a number of commercial digital cameras. Numerous other media can be practiced without departing from the scope and spirit of the invention. The recording/transmission module 108 can be implemented to transmit the output signal 116 to an external device or location. For example, the output signal 116 can be transmitted by an infra-red transmitter built into the recording device 100 to a corresponding receiver in another device such as a computer. Alternatively, it can be transmitted electrically via an appropriate interface built into the device 100 via one or more conductors to an external device and then to the Internet or an Intranet. The foregoing are merely indicate a few of the many ways of transmitting information between two devices that can be practiced. The watermarked photo 116 can be sent to John's representative so that the photo can be immediately used by various news agents. Preferably, the communication of the photo from the recording/transmission module 108 is via a wireless communication network. Optionally, registration information about the digital photo 116 can also be sent to a service center if necessary.

In the foregoing embodiment of the invention, the functionality of each module 102, 104, 106, and 108 can be implemented as an electronic circuit. Alternatively, at least part of the functionality of each module may be implemented as a computer program

that is carried out by a microprocessor coupled to appropriate storage means, both forming part of the recording device 100. Numerous audio, image and video capture devices are implemented utilising microprocessors and other forms of computer systems. For example, the watermarking module 106 can be implemented entirely as software executing on a microprocessor in the recording device 100. Analogously, the authentication module can be implemented using an appropriate sensing or coupling device to obtain a required external signal or information in conjunction with software executing on a microprocessor to carry out the remaining functionality of the module or a portion thereof.

A flowchart illustrating the method for generating an authenticated audio, image and/or video signal in accordance with the second embodiment is depicted in Fig. 2. Processing commences in step 200. In step 202, a check is made to determine if the operator is authorised, and if so authentication data is generated. In step 204, image, video, and/or audio data is captured if the operator is authorised. Steps 202 and 204 may be performed substantially simultaneously without departing from the scope and spirit of the invention. In step 206, the captured audio, image and/or video signal is watermarked with the authentication data. For further details of specific steps to be carried out, reference is made to the functionality of the apparatus of the first embodiment described above with reference to Fig. 1.

An apparatus in accordance with a third embodiment of the invention is depicted in Fig. 3. Features of the first embodiment that have corresponding parts in the third embodiment are denoted with a corresponding reference numeral. Thus, the authentication module 102 of Fig. 1 is denoted with reference numeral 302 in Fig. 3. For the purpose of brevity in the description, reference is simply made to the description of those corresponding modules in the description hereinbefore and not repeated here. Only the new elements of Fig. 3 are described in detail hereinafter. While the third embodiment illustrates two additional modules 318 and 320, it will be appreciated by one skilled in the art that the embodiment can be practiced optionally with only one of the two modules.

The recording device 300 includes a global positioning system (GPS) module 320 that can obtain accurate positioning information about the location of the recording device 324 when in operation. The GPS data 324 may be obtained at a predetermined instance or interval to be embedded in the captured signal 314 by the watermarking module 306. For example, after the operator is authenticated as authorised to operate the recording device 300 and when the capture module 304 is actuated, the GPS module 320 may obtain fresh GPS data or retrieve most recently stored GPS data to be provided as output 324 to the watermarking module 306.

Further, the recording device 300 can include an annotation module 318. The annotation module annotation module 318 can add annotation text, voice, or links to other media-segments directly into the media signal produced by the capture module 304 in a conventional manner. The annotation can be persistent and/or non-persistent. For example, a microphone and/or text input device can be included in the recording device 300 as part of the annotation module 318 for annotation purpose. Annotation information can be stored together with the media data based on a standard data format. For example, in the case of video media, the MPEG2 standard can be used which provides space for annotation. This is non-persistent annotation. Alternatively or in addition to non-persistent annotation, persistent annotation can be incorporated into the captured media signal 314.

The annotation module 318 also provides annotation signal 322 to the watermarking module 306. To make the annotation persistent, watermarking is used again to embed the annotation information 322 into the media data 314. Such persistent annotation can be either perceivable or non-perceivable. For example, persistent annotation is useful to put particular information at a particular location of an image. Alternatively, it can be used to put information in a particular interval of audio for indication of information like "this is John" or "sang by Linda". Therefore, the persistent and non-persistent annotation is useful to specify messages to be embedded in a captured media

signal, as well as information such as the location or time period which can be embedded in the media signal.

The foregoing embodiments of the invention disclose a method, apparatus and computer program product for generating an authenticated audio, image and/or video signal, where the authenticated signal is an audio, image and/or video signal watermarked with authentication data. The embodiments of the invention are advantageous in that they ameliorate or overcome one or more disadvantages of conventional audio, image and video capture systems. In particular, the embodiments of the invention are able to do so by requiring authentication data derived from an operator to operate a recording device and providing on-the-fly copyright ownership indicia in a recording by watermarking the recording using the authentication data. This is done in the recording device that is used to capture the audio, image and/or video work.

A small number of embodiments have been disclosed by way of example. However, those skilled in the art will recognise that the invention can be practiced, with modification, in the light of the information contained herein without departing from the scope and spirit of the invention.

The claims defining the invention are as follows:

1. A method of generating an authenticated audio, image and/or video signal, including:

generating an authentication signal;

capturing a digital audio, image and/or video signal; and

watermarking said digital audio, image and/or video signal using said authentication signal to provide said authenticated audio, image and/or video signal.

2. The method according to claim 1, wherein said step of generating said authentication signal is performed substantially simultaneously with said step of capturing said digital audio, image and/or video signal.

3. The method according to claim 1 or 2, wherein said authentication signal is derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

4. The method according to any one of claims 1 to 3, wherein said step of capturing said digital audio, image and/or video signal includes:

capturing an analog audio, image and/or video signal; and

converting said analog audio, image and/or video signal to said digital audio, image and/or signal.

5. The method according to any one of claims 1 to 4, wherein said watermarking step provides perceptible and/or non-perceptible watermarks.

6. The method according to any one of claims 1 to 5, further including the step of annotating said digital audio, image and/or video signal using text and/or audio data.

7. The method according to any one of claims 1 to 6, wherein said annotating step is persistent and/or non-persistent.

8. The method according to any one of claims 1 to 7, further including the steps of:

determining if an operator is authorised to generate said authenticated audio, image and/or video signal; and

if so, enabling capture of said digital audio, image and/or video signal.

9. An apparatus for generating an authenticated audio, image and/or video signal, including:

means for generating an authentication signal;

means for capturing a digital audio, image and/or video signal; and

means for watermarking said digital audio, image and/or video signal using said authentication signal to provide said authenticated audio, image and/or video signal.

10. The apparatus according to claim 9, wherein said means for generating said authentication signal operates substantially simultaneously with said means for capturing said digital audio, image and/or video signal.

11. The apparatus according to claim 9 or 10, wherein said authentication signal is derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

12. The apparatus according to any one of claims 9 to 11, wherein said means for capturing said digital audio, image and/or video signal includes:

means for capturing an analog audio, image and/or video signal; and

means for converting said analog audio, image and/or video signal to said digital audio, image and/or signal.

13. The apparatus according to any one of claims 9 to 12, wherein said means for watermarking provides perceptible and/or non-perceptible watermarks.

14. The apparatus according to any one of claims 9 to 13, further including means for annotating said digital audio, image and/or video signal using text and/or audio data.

15. The apparatus according to any one of claims 9 to 14, wherein said means for annotating provides persistent and/or non-persistent annotation.

16. The apparatus according to any one of claims 9 to 15, further including:

means for determining if an operator is authorised to generate said authenticated audio, image and/or video signal; and

means for enabling capture of said digital audio, image and/or video signal in response to determining said operator is authorised.

17. A computer program product having a computer readable medium having a computer program recorded therein for generating an authenticated audio, image and/or video signal, said computer program product including:

means for generating an authentication signal;

means for capturing a digital audio, image and/or video signal; and

means for watermarking said digital audio, image and/or video signal using said authentication signal to provide said authenticated audio, image and/or video signal.

18. The computer program product according to claim 17, wherein said means for generating said authentication signal operates substantially simultaneously with said means for capturing said digital audio, image and/or video signal.

19. The computer program product according to claim 17 or 18, wherein said authentication signal is derived from biometrics data, a password, user identification

data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

20. The computer program product according to any one of claims 17 to 19, wherein said means for capturing said digital audio, image and/or video signal includes:

means for capturing an analog audio, image and/or video signal; and

means for converting said analog audio, image and/or video signal to said digital audio, image and/or signal.

21. The computer program product according to any one of claims 17 to 20, wherein said means for watermarking provides perceptible and/or non-perceptible watermarks.

22. The computer program product according to any one of claims 17 to 21, further including means for annotating said digital audio, image and/or video signal using text and/or audio data.

23. The computer program product according to any one of claims 17 to 22, wherein said means for annotating provides persistent and/or non-persistent annotation.

24. The computer program product according to any one of claims 17 to 23, further including:

means for determining if an operator is authorised to generate said authenticated audio, image and/or video signal; and

means for enabling capture of said digital audio, image and/or video signal in response to determining said operator is authorised.

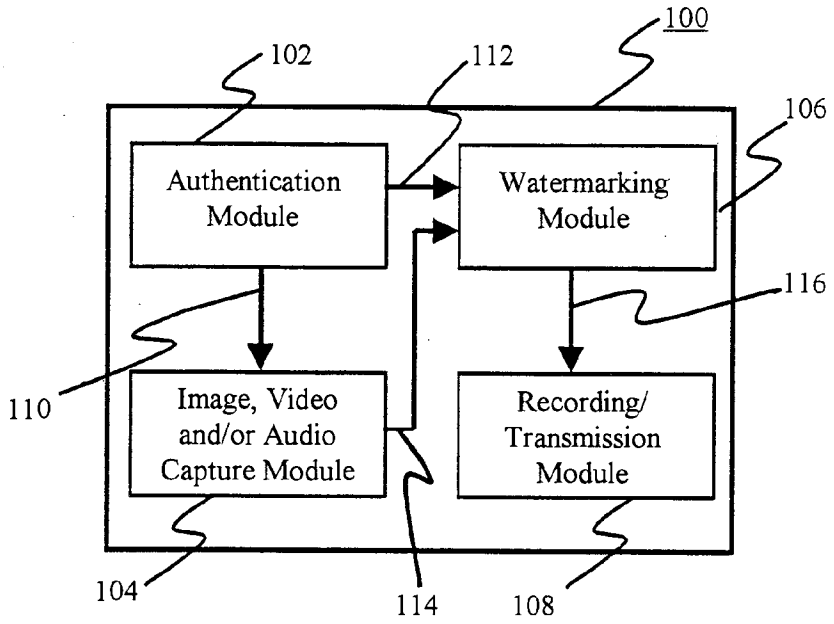

100
102
112
106
Authentication Module
Watermarking Module
116
110
Image, Video and/or Audio Capture Module
Recording/ Transmission Module
104
114
108

FIG. 1

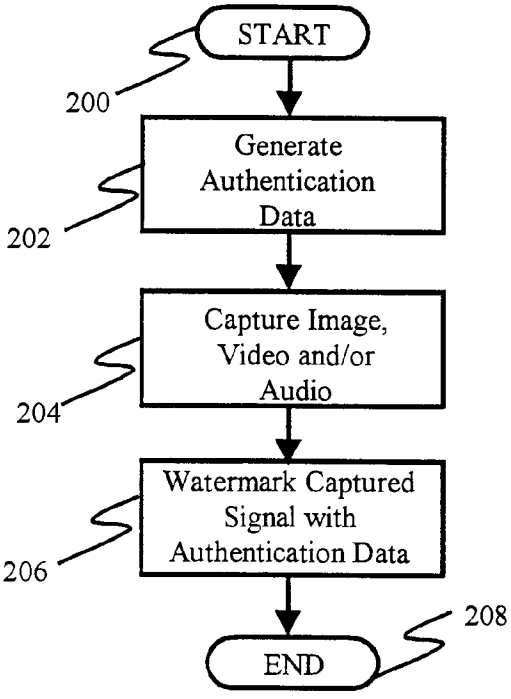

START
200
Generate Authentication Data
202
Capture Image, Video and/or Audio
204
Watermark Captured Signal with Authentication Data
206
208
END

FIG. 2

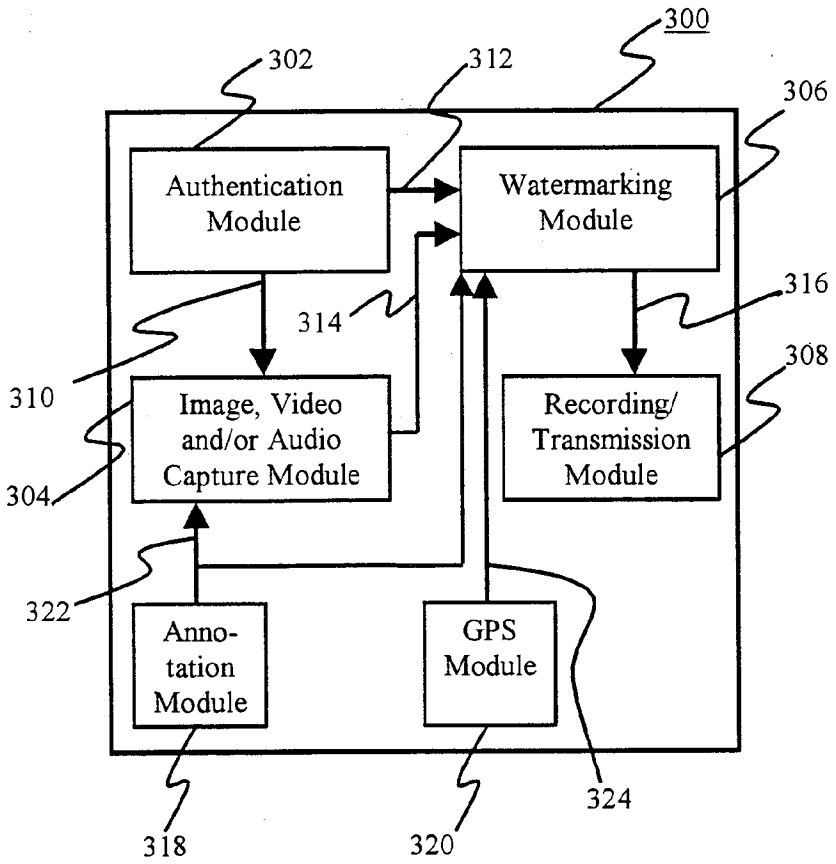

300
302
312
306
Authentication Module
Watermarking Module
316
314
310
308
Image, Video and/or Audio Capture Module
Recording/ Transmission Module
304
322
Anno-tation Module
GPS Module
324
318
320

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 98/00104

A. CLASSIFICATION OF SUBJECT MATTER

IPC[6]: G 11 B 23/28, 23/36, 23/40

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[6]: G 11 B 23/00; H 04 N 5/00, 7/00; G 07 C 9/00; H 04 L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96/03 835 A2 (MACROVISION CORP.), 08 February 1996 (08.02.96), fig.1-3; abstract; claim 1.	1-5,9-12
A	EP 0 779 602 A2 (AT & T CORP.), 18 June 1997 (18.06.97), fig.1,4; abstract; claim 1.	1-16
A	US 5 598 473 A (LINSKER et al.), 28 January 1997 (28.01.97), abstract; fig.1,2; claim 1.	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed
„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 January 1999 (25.01.99)	01 September 1999 (01.09.99)

Name and mailing adress of the ISA/AT	Authorized officer
Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/200	Berger Telephone No. 1/53424/453

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 98/00104

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 17 to 24
because they relate to subject matter not required to be searched by this Authority, namely:
the features of these claims 17 to 24 disclose a computer program.

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG 98/00104

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
WO A2 9603835	08-02-96	AU A1 31276/95	22-02-96
		AU B2 697727	15-10-98
		BR A 9508340	09-09-97
		CA AA 2195939	08-02-96
		CN A 1159272	10-09-97
		EP A2 775418	28-05-97
		JP T2 10503338	24-03-98
		NZ A 290521	28-10-98
		US A 5574787	12-11-96
		WO A3 9603835	04-04-96
EP A2 779602	18-06-97	CA AA 2188975	16-06-97
		JP A2 9179583	11-07-97
		US A 5761329	02-06-98
US A 5598473	28-01-97	US A 5680455	21-10-97